



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/406,087	09/24/1999	RYOTA AKIYAMA	1341.1030/JD	1217

21171 7590 11/07/2003

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 11/07/2003

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/406,087

Applicant(s)

AKIYAMA ET AL.

Examiner

Christopher J. Brown

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 May 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 September 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6. 6) ☐ Other: _____

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: On page 4 line 22 "other the" is not correct, the examiner believes the applicant to mean "the other". On page 8 line 17, a verb is missing in the statement "using keys K1 to Kn to authentication signs CS1 to CSn respectively," the examiner suggests "create".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4 and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear whether "each other" refers to the first authenticator creating unit and second authenticator creating unit, or first authenticator and second authenticator. The examiner has interpreted the claim as "each other" referring to the first authenticator and second authenticator. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1,2, 4-6, and 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis US 5,907,619 in view of Bellare US 5,757,913.

4. As per claims 1, 6, and 11, Davis discloses an authentication system comprising a signing station (secure compressed signing device) that creates an authenticator by applying a one way function (hash function), (Col 5 lines 10-30).

Davis discloses a certifying station (receiving device) for checking the authentication of the information, (Col 3 lines 54-61)

Davis discloses that the first authenticator creating unit divides the information into a plurality of data, and creating a plurality of authenticators (hashes) by applying a different one way function to each data, (Col 5 lines 15-27).

Davis discloses a linking unit for linking the plurality of authenticators created (hash table), (Col 5 lines 36-42).

Davis discloses that the certifying station (receiving device) has a separating unit to create authenticators of said divided data and comparing the authenticators created with the authenticators sent from the signing station to authenticate the data, (Col 6 lines 1-14).

Davis does not disclose that the signature (hash) is appended to the information.

Bellare discloses that the information is signed with an authenticator, (MAC) (Col 3 lines 48-60).

It would be obvious to modify Davis's authentication system, with Bellare's signing methods to make certain that the authenticator belongs to the data sent.

Art Unit: 2134

As per claims 2, and 7, Davis discloses truncating (hashing) the authenticators created by said first authenticator creating unit, (Col 5 lines 35-41). Davis discloses said certifying unit compares the authenticators to check for authentication of the information, (Col 5 lines 53-56, Col 6 lines 1-14).

As per claims 4, and 9, Davis discloses a signing station, and a certifying station.

Davis does not disclose parallel processing.

Bellare discloses parallel processing, (Col 1 lines 60-65).

It would be obvious to one skilled in the art to modify Davis's authentications system with Bellare's parallel processing because it increases production speed.

As per claims 5, and 10, Davis discloses that both the first and second authenticator units use intermediate data from the first authenticator, to create a second authenticator, (hash of the hash table), (Col 5 lines 35-40).

Claims 3, 8, and 12-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis US 5,907,619 in view of Bellare US 5,757,913 in view of Rogaway US 5,651,069.

5. As per claims 3, 8, and 12-23 Davis-Bellare discloses an authentication system comprising a signing station (secure compressed signing device) that creates an authenticator by applying a one way function (hash function), (Col 5 lines 10-30).

Davis discloses a certifying station (receiving device) for checking the authentication of the information, (Col 3 lines 54-61). Davis discloses an authentication system with a number of different one way functions, (Davis Col 5 line 24).

Art Unit: 2134

Davis discloses that the first authenticator creating unit divides the information into a plurality of data, and creating a plurality of authenticators (hashes) by applying a different one way function to each data, (Col 5 lines 15-27).

Davis discloses a linking unit for linking the plurality of authenticators created (hash table), (Col 5 lines 36-42). Davis discloses that the certifying station (receiving device) has a separating unit to create authenticators of said divided data and comparing the authenticators created with the authenticators sent from the signing station to authenticate the data, (Col 6 lines 1-14). Davis discloses that both the first and second authenticator units use intermediate data from the first authenticator, to create a second authenticator, (hash of the hash table), (Col 5 lines 35-40). Bellare discloses that the information is signed with an authenticator, (MAC) (Col 3 lines 48-60).

Davis-Bellare does not disclose a key

Rogaway discloses a one way function based on a secret key, (Col 1 lines 63-67, Fig 3).

It would be obvious to one skilled in the art to modify the Davis Bellare combination with Rogaway's key method, because in addition to verifying that the document has not been tampered with, the secret key method authenticates the sender thus increasing security, (Rogoway Col 5 lines 45-50).

Conclusion


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J Brown whose telephone number is 703-305-8023. The examiner can normally be reached on 8:30-6:00.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Christopher J. Brown

10/23/03



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100